AO 106 (Rev. 04/10) Application for a Search Warrant AUTHORIZED AND APPROVED/DATE: JLG 5/20/25

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT leeclark64@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC

Case No. M-25-352-SM

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, which is attached and incorporated by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(5)(B) and (b)(2)	Possession of and/or Access with Intent to View Material Containing Child Pornography (or attempting the same)

The application is based on these facts:
See attached Affidavit of Special Agent Timothy Doyle, Federal Bureau of Investigation, which is incorporated by reference herein.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Timothy Doyle, SA
Printed name and title

Sworn to before me and signed in my presence.

Date: May 28, 2025

Judge's signature

City and state: Oklahoma City, Oklahoma

Suzanne Mitchell, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT **leeclark64@gmail.com** THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. M-25-352-SM

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Timothy Doyle, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application for a search warrant for information associated with email account leeclark64@gmail.com ("the Subject Account"), stored at premises controlled by Google LLC ("Google"), an electronic communications and remote computing service provider headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the FBI and have been so employed since approximately September 2015. I am currently assigned to the FBI's Oklahoma City Field Office, Stillwater Resident Agency. As part of my duties as an FBI Special Agent, I investigate federal criminal violations, to include child exploitation and abuse violations. As a result of my training and experience, including information provided by other federal agents with applicable knowledge, I am familiar with the tactics, methods, and techniques used by criminals in cases such as this. As part of my job, I have conducted numerous investigations involving the use of the internet, smart phones, email, and social media to further criminal activity. I have participated in the execution of multiple federal search warrants involving various types of evidence and property.

3. The information contained in this Affidavit is based on, among other things, my participation in the investigation described herein, my review of the relevant documents and files, information obtained from law enforcement officers and others, and knowledge gained from my training and experience. Because I submit this Affidavit for the limited purpose of establishing probable cause, it does not set forth all of my knowledge about this matter.

4. Based on my training and experience, and the facts set forth in this Affidavit, I submit that there is probable cause to believe that Lee Grant Clark has committed violations of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Possession of and/or Access with Intent to View Material Containing Child Pornography (or attempting the same). I further submit that there is probable cause to search the Subject Account further described in

Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes, as further described in Attachment B. The FBI submitted a preservation request for the Subject Account to Google on May 7, 2025.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense[s] being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. During the course of an investigation into violations of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Possession of and/or Access with Intent to View Material Containing Child Pornography (or attempting the same), and 18 U.S.C. § 2252A(a)(2)(A) and (b)(1), Receipt of Child Pornography (or attempting the same), the FBI identified Lee Grant Clark, resident of 1109 S Lewis, Stillwater, OK 74074 (the SUBJECT PREMISES) as a primary suspect. After confirming Clark resided at the SUBJECT PREMISES, the FBI obtained a federal search warrant for the SUBJECT PREMISES, which included the search of electronic devices seized from the SUBJECT PREMISES. This warrant was executed on May 6, 2025. There were no indications of anyone other than Clark living at the SUBJECT PREMISES.

7. Prior to the execution of the warrant, the FBI received from Stillwater Police Department a report regarding Jane Doe 1, who reported that Clark sexually abused her

around 2004 when she was around 10-years-old. She further reported Clark also abused Jane Doe 2, who was then a minor, on repeated occasions. Jane Doe 1's report included allegations that Clark took pictures of Jane Doe 1 and Jane Doe 2.

8. During the execution of the warrant, the FBI seized Clark's T-Mobile Revvl V cellular phone.[1] The FBI's Computer Analysis Response Team (CART) began previewing it on-scene. Some images of child sexual abuse material (CSAM) were located on the phone in a locally stored pictures folder. Those include the following: In the filepath of Dump\data\media\0\Pictures\Nudes\20210628_193749.jpg is a photo of what appears to be young girl around 13-15 years of age. She is completely nude and laying down with arms and legs spread with both breasts and genitals exposed. There is another photo at file path Dump\data\media\0\Pictures\Nudes\20210628_193038.jpg depicting what appears to be a different young girl around 13-15 years of age. This girl is completely nude standing facing the camera with both breasts and genitals exposed. Multiple images were also found in the Google Photos Cache depicting what appears to be nude minor females appearing to be 15-16 years old.

9. Additional review of the cellular phone located the Google account of leeclark64@gmail.com as the primary account for the cellular phone described above. The apps for Google Photos, Gmail, Google Calendar, Google Meet, Google Maps, and Google Play, along with other Google apps, were located on the device. An initial review of the

[1] To my knowledge, this phone was not manufactured in Oklahoma.

Gmail account shows an email from leeclark64@gmail.com to abuse@easynews.com wherein Clark is complaining that a message board located at Alt.Binary.Pictures.PureBeauty is allowing persons to flood the group with pics such as "adult black models" that are hindering legitimate posters trying to "post appropriate pics of 'Pure Beauty' which is young teen and children models". Further review of the phone revealed the Google Chrome Tab History to contain artifact information for pornography URLs with titles to include: The Kristen Archives – Just Incestuous Stories, The Young Girl Erotica Repository (TYGER) Story Index, and Lesbian Lolita – Unfastened Belts. Based on my training and experience, "Loli" is a common term used to refer to child pornography.

10. Clark's computer, which was a NZXT, model CATH500BTW1, S/N: 01184666703612, was also seized. Dontknowdoya is the user name for this computer. The computer could only be partially reviewed while at the SUBJECT PREMISES. Items located on the partial review included the Documents Folder, wherein there is a subfolder named stories, and within this subfolder are additional subfolders named: incest; Loliwood_rip; Loliwood_rip_by_title; MrDoubles stories; PocketFiles; and Twin Sisters. The folder named incest contains writings from authors that discuss: 2rape2.txt – Rape of the persons Mother and Sister; Badboyc2.txt – sexual-based chat message between a 13-year-old bisexual girl and 6-year-old sister; incestuo.txt – A story about a father on vacation with his 13 year-old daughter and their baby, and the father having sex with both of them. The folder Loliwood_rip contains 280+ writings describing sex with minors and incest

from LoliwoodStudios: Child Erotica at its Best. An image was also located with filename: vlcsnap-2025-04-29-17h20m05s992.png, located at \root\home\dontknowdoya\Pictures\. This is a picture of two nude adolescent girls facing each other. The child on the left side of the picture is suspected to be between the ages of 11 and 14 and has her right breast and nipple exposed. The child on the right side of the picture is suspected to be between 7 to 10 years old and can be seen naked from her thighs up. The upper portion of her vulva is exposed and in plain view.

11. Some of the indicators of ownership on the computer included a file named MyHealthVet.txt, which lists the login information for MyHealthVet, with the username leeclark64. Additionally, CART located another file named MyPay.txt, which contained login information, including a username of leeclark64@gmail.com.

12. Additionally, in a cached folder on the computer, CART located several CSAM files. For example, one image depicted a prepubescent female, who was completely nude and laying on a bed, and she had her legs spread so that her genitals were exposed. The "last modified" date on this image is April 17, 2025. Another image depicted a minor female with her mouth and tongue touching an adult male's penis.

13. Agents also found numerous discs and tape recordings in the SUBJECT PREMISES. Some, but not all, have been previewed. The discs and tape recordings revealed footage of minor girls, to include Jane Doe 2. The recordings appeared to show Jane Doe 2 and several of her friends running around the home acting silly, laying on their beds, and singing and dancing while someone was filming them. Some of the discs also

include photos of at least one girl asleep. While the girl was fully clothed, some of the photos were zoomed in on her buttocks.

14. Finally, agents found printed, typed stories in the SUBJECT PREMISES that would constitute child erotica. One story, titled "Private Lessons," features Jane Doe 2 as the main character and refers to her by first and last name. Another story is told from the point of view of a father engaged in a sexual relationship with his daughter and her friend, and the father is concerned both are pregnant.

15. Clark was arrested following the execution of the warrant.

16. Since Clark's arrest, the FBI has spoken with or reviewed documentation regarding multiple other females who reported that Clark sexually abused them as children. For example, in 1999, two minor females reported Clark, who was then a neighbor of one of the girls, sexually abused them in 1999, such as by having them spread their legs while wearing skirts and showing them pornography. Additionally, an adult female indicated to the FBI that she was sexually abused by Clark in 1980, when she was around 8-years-old. She explained how Clark touched her vagina and told her she could not tell anyone.

17. Based on my training and experience, evidence of an attraction to minors can serve as supporting evidence that an individual knowingly possessed child pornography. The warrant I am applying for thus seeks to seize not only information related to child pornography, but also information related to child erotica and to minors who, even if not depicted in child pornography, may have been used by Clark for sexual satisfaction.

18. Further, based on open-source research, Google was founded in 1998. Any Google accounts, then, must have been created in or after 1998. Because this investigation has revealed child sexual abuse by Clark that dates back to 1980, including one instance in 1980 and another instance in 1999, the warrant I am applying for seeks data from the date of Clark's account creation until the date Clark was arrested, May 6, 2025.

BACKGROUND CONCERNING GOOGLE[2]

19. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

20. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of

[2] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

21. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

22. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

23. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

24. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by

manually creating a group within Google Contacts or communicating with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

25. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

26. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the

user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

27. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

28. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile

phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

29. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

30. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like

latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

31. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

32. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout,

Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

33. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

34. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated

with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

35. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

36. In my training and experience, evidence of who was using a Google account and from where, and evidence related to possessing or accessing with intent to view child pornography, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

37. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

38. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of

occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

39. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

40. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

41. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

42. Based on the forgoing, I request that the Court issue the proposed search warrant.

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

TIMOTHY DOYLE
SPECIAL AGENT
FBI

Subscribed and sworn to before me on May 28, 2025.

SUZANNE MITCHELL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Google account **leeclark64@gmail.com** ("Subject Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC. ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on 05/07/2025 with the Google Reference Number 92773667, Google is required to disclose to the government for the Subject Account listed in Attachment A the following information from **the date of the account's creation through May 6, 2025**, unless otherwise indicated:

1. All business records and subscriber information, in any form kept, pertaining to the Account, including:

    i. Names (including subscriber names, user names, and screen names);
    ii. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
    iii. Telephone numbers, including SMS recovery and alternate sign-in numbers;
    iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
    v. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers;

vi. Length of service (including start date and creation IP) and types of service utilized;
vii. Means and source of payment (including any credit card or bank account number); and
viii. Change history.

2. All device information associated with the Subject Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

3. Records of user activity for each connection made to or from the Subject Account, including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs;

4. The contents of all emails associated with the Subject Account, including stored or preserved copies of emails sent to and from the Subject Account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

5. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

6. The contents of all text, audio, and video messages associated with the Subject Account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

7. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

8. The contents of all records associated with the Subject Account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, applications, and other data uploaded, created, stored, or shared with the Subject Account including drafts and deleted records; third-party application data and backups; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

9. The contents of all media associated with the Subject Account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the Subject Account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

10. All maps data associated with the Subject Account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the Subject Account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

11. All Location History and Web & App Activity indicating the location at which the Subject Account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;

12. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history;

13. Subscriber information for any accounts linked to the Subject Account by recovery email, secondary email, SMS recovery number, and/or cookie, to include, full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the linked account was created, the length of service, the IP address used to register the linked account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

14. All accounts that share a browser cookie with the Subject Account, and any associated details, such as the time the cookie was associated with the Subject Account; and

15. Any and all cookies or cookie data specific to the Subject Account.

Google is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Possession of and/or Access with Intent to View Material Containing Child Pornography (or attempting the same), by Lee Grant Clark, including, for the Subject Account listed on Attachment A, information pertaining to the following matters:

a. Evidence of the possession, viewing, receiving, distributing, purchasing, producing, or accessing of child pornography, including, but not limited to, any files, communications, or user activities that involve or relate to child pornography or child erotica;

b. Evidence of the identities of any minors that may be depicted in child pornography possessed by Lee Grant Clark or that may have been otherwise used or abused by Clark for sexual satisfaction;

c. Evidence indicating how, where, and when the Subject Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner, including metadata associated with any files subject to seizure;

d. Evidence indicating the Subject Account owner's state of mind as it relates to the crime under investigation;

e. The identity of the person(s) who created or used the Subject Account;

f. The identity of the person(s) who communicated with the Subject Account about matters relating to violations of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Possession of and/or Access with Intent to View Material Containing Child Pornography (or attempting the same), including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data

may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.